PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

PCT/FI99/00565

Helsinki 18.08.99

09/743302

REC'D 22 SEP 1999
WIPO PCT

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

Hakija Applicant	NOKIA TELECOMMUNICATIONS OY Helsinki
Patenttihakemus nro Patent application no	981565
Tekemispäivä Filing date	07.07.98
Kansainvälinen luokka International class	H 04L
Keksinnön nimitys Title of invention	"Autentikointi tietoliikenneverkossa"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A
Address: P.O.Box 1160
FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5204
Telefax: + 358 9 6939 5204

23

Autentikointi tietoliikenneverkossa

Keksinnön ala

Keksintö liittyy autentikointiin tietoliikenneverkossa, erityisesti IP-verkossa (IP=Internet Protocol) ja lisäksi verkon tietoturvaominaisuuksien parantamiseen suoritetun autentikoinnin avulla. Autentikoinnilla tarkoitetaan tietoa generoineen osapuolen, kuten tilaajan, identiteetin todennusta. Autentikoinnin avulla voidaan myöskin taata kyseisen tiedon eheys (integrity) ja luottamuksellisuus (confidentiality). Autentikointi voidaan suorittaa erilaisia tarkoitusperiä, kuten verkkopalvelujen käyttöoikeuksien tarkistamista varten. Keksintö on tarkoitettu käytettäväksi erityisesti liikkuvien päätelaitteiden yhteydessä, mutta keksinnön mukaisella ratkaisulla saavutetaan etuja myös kiinteiden päätelaitteiden yhteydessä.

Keksinnön tausta

Eräs viime vuosien merkittävimpiä viestintään liittyviä ilmiöitä on ollut Internet-käyttäjien voimakas kasvu. Nopea kasvu on myös nopeasti tuonut esiin Internetin puutteita. Eräs näistä on verkon heikko tietoturva. Nykyisin yleisesti käytössä oleva IP-protokollaversio (IPv4) ei tarjoa välineitä, joilla voitaisiin varmistaa, että vastapäästä tullut informaatio ei muuttunut siirron aikana tai että informaatio ylipäätään tuli siltä lähteeltä, joka väittää lähettäneensä ko. informaation. Lisäksi verkossa on helppo käyttää erilaisia työkaluja, joilla voidaan kuunnella liikennettä. Tästä johtuen ovat mm. sellaiset järjestelmät, jotka lähettävät salaamattomana kriittistä informaatiota, esim. salasanoja, erittäin haavoittuvia.

IP:n uudessa versiossa (IPv6) on sisäisesti ominaisuuksia, jotka mahdollistavat turvallisen kommunikoinnin Internet-käyttäjien välillä. Koska muutos uuteen protokollaan tulee olemaan hidas, tietoturvaominaisuuksien tulee olla sellaisia, että ne ovat yhteensopivia nykyisen IP-version (IPv4) kanssa ja lisättävissä siihen.

Internetin tietoturvaominaisuuksien parantamiseksi on kehitetty erilaisia järjestelmiä, joiden avulla käyttäjät voivat lähettää tiedon salattuna vastakkaiselle osapuolelle. Eräs tällainen järjestelmä on Kerberos, joka on palvelu, jonka avulla verkon käyttäjät ja palvelut voivat autentikoida toisensa ja jonka avulla käyttäjät ja palvelut voivat luoda väliinsä salattuja yhteyksiä. Kerberos-järjestelmää käytetään hyväksi esillä olevan keksinnön eräässä toteutustavas-

sa, jota kuvataan tarkemmin jäljempänä.

Toinen nykyisin vaikuttava suuntaus on erilaisten liikkuvien päätelaitteiden voimakas yleistyminen. Tämän kehityksen myötä on entistä tärkeämpää, että päätelaitteet saavat liitynnän (access) dataverkkoon myös silloin, kun he ovat kotiverkkonsa ulkopuolella. Tällainen liityntä voi oleellisesti parantaa esim. kannettavan tietokoneen käytettävyyttä silloin, kun käyttäjä ei ole tavanomaisessa työympäristössään. Liityntäpisteitä voi olla esim. lentokentillä, rautatieasemilla, ostoskeskuksissa tms. julkisissa tiloissa ja liityntä voi tapahtua langallisesti tai langattomasti.

Edellä mainitun kaltaiset järjestelmät, joiden avulla voidaan lähettää salattua tietoa osapuolien välillä on tarkoitettu lähinnä kiinteille päätelaitteille ja ne edellyttävät, että käyttäjät ovat etukäteen rekisteröityneet palvelun käyttäjiksi. Ongelmana nykyisin onkin se, että päätelaitteiden liikkuvuutta tukeville IP-verkoille ei ole olemassa toimivaa autentikointi- tai avaimienhallintajärjestelmää, joka takaisi hyvän maantieteellisen kattavuuden ja mahdollistaisi samalla sen, että käyttäjä voi helposti saada autentikoidun ja turvallisen yhteyden käyttöönsä maantieteellisesti mahdollisimman laajalla alueella.

Keksinnön yhteenveto

Keksinnön tarkoituksena on päästä eroon edellä kuvatusta epäkohdasta ja saada ratkaisu, jonka avulla tietoliikenneverkon, kuten IP-verkon käyttäjät saadaan autentikoitua yksinkertaisesti ja joustavasti lähes riippumatta siitä, missä päin heidän kulloinenkin verkkoliityntäpisteensä sijaitsee maantieteellisesti.

Tämä päämäärä saavutetaan ratkaisulla, joka on määritelty itsenäisissä patenttivaatimuksissa.

Keksinnössä hyödynnetään olemassa olevan matkaviestinverkon, erityisesti GSM-verkon (Global System for Mobile Communications), autentikointimenetelmää IP-verkossa (tai muussa matkaviestinverkkoon nähden erillisessä verkossa). Tämä tarkoittaa sitä, että IP-verkon käyttäjä käyttää IP-verkon päätelaitteessaan samaa (tai oleellisesti samanlaista) tilaajan tunnistusyksikköä (SIM-korttia) kuin matkapuhelimessaan tai -viestimessään. Ajatuksena on hakea tilaajan autentikointitiedot matkaviestinverkosta IP-verkon puolelle ja suorittaa autentikointi näiden tietojen perusteella IP-verkossa. Matkaviestinverkko ei välttämättä ole GSM-verkko, vaan se voi olla jokin muukin matkaviestinverkko, jossa autentikointia käytetään oleellisesti samalla

tavalla, esim. DCS-verkko (Digital Cellular System), GPRS-verkko (General Packet Radio Service, joka on GSM:n aliverkko) tai UMTS-verkko (Universal Mobile Telecommunications System).

Keksinnön erään edullisen toteutustavan mukaisesti käyttäjä rekisteröidään, vasteena onnistuneelle autentikoinnille, erilliselle avaimienhallintajärjestelmälle, edullisesti Kerberos-järjestelmälle, jolloin keskenään kommunikoivien käyttäjien välille pystytään tämän jälkeen helposti luomaan salattu kanava. Tämä on tärkeätä erityisesti silloin, kun ainakin osa siirtoyhteydestä muodostuu radiotiestä.

Keksinnön mukaisen ratkaisun ansiosta IP-verkon käyttäjät saadaan autentikoitua helposti ja joustavasti ja käyttäjät pystyvät lisäksi saamaan tehokkaat turvaominaisuudet käyttöönsä maantieteellisesti laajalla alueella. Tämä johtuu toisaalta GSM-verkkojen laajasta levinneisyydestä ja toisaalta siitä, että operaattorien väliset roaming-sopimukset mahdollistavat vieraaseen verkkoon tulevien tilaajien autentikoinnin. Esim. eräällä suomalaisella GSM-operaattorilla on tällä hetkellä (1998) yhteisliikennesopimuksia yli 60 maassa toimivien operaattorien kanssa.

Keksinnön mukaisen ratkaisun ansiosta ISP-operaattorien (Internet Service Provider), jotka tarjoavat tyypillisesti myös matkaviestinpalveluja, ei tarvitse erikseen hankkia autentikointi- ja avaimienhallintajärjestelmiä IP-verkkoon, vaan he voivat hyödyntää operoimansa matkaviestinverkon ominaisuuksia myös tähän tarkoitukseen.

Keksinnön mukaisella ratkaisulla saavutetaan kiinteiden päätelaitteiden yhteydessä myös sellainen etu, että matkaviestinverkon yhteyteen rakennettuja toimintoja voidaan käyttää hyväksi Internet-palvelujen yhteydessä. Esim. organisaatio, joka toimii sekä matkaviestinoperaattorina että ISP-operaattorina voi hyödyntää matkaviestinverkon yhteyteen rakennettuja laskutuspalveluja laskuttaakseen Internet-palvelujen tarjoamisesta. Kun kiinteätkin päätelaitteet autentikoidaan keksinnön mukaisella menetelmällä, saavutetaan suuri varmuus siitä, että lasku kohdistuu oikeaan tilaajaan. Lisäksi tilaaja saadaan autentikoitua, vaikka hän kytkeytyisi verkkoon vieraalta päätelaitteelta.

Kuvioluettelo

Seuraavassa keksintöä ja sen edullisia toteutustapoja kuvataan tarkemmin viitaten kuvioihin 1...10 oheisten piirustusten mukaisissa esi-

merkeissä, joissa

kuvio 1 havainnollistaa erästä keksinnön mukaisen menetelmän toimintaympäristöä,

kuvio 2 esittää eri elementtien välillä käytävää sanomanvaihtoa, kun päätelaite kytkeytyy verkkoon tai irrottautuu verkosta,

kuvio 3 havainnollistaa niiden sanomien rakennetta, joiden avulla ilmoitetaan järjestelmän palvelimelle, että käyttäjä on kytkeytynyt verkkoon tai irrottautunut verkosta,

kuvio 4 esittää autentikoinnin aikana eri elementtien välillä käytävää sanomanvaihtoa,

kuvio 5 havainnollistaa kuvion 5 sanomien yleistä rakennetta,

kuvio 6 havainnollistaa järjestelmän niitä elementtejä, joilla hankitaan yhteyskohtainen salausavain kahden päätelaitteen välille,

kuvio 7 esittää sanomanvaihtoa, joka käydään aloituspääsylipun saamiseksi Kerberos-palvelimelta,

kuvio 8 havainnollistaa päätelaitteen keksinnön kannalta oleellisia osia,

kuvio 9 esittää sanomanvaihtoa, joka käydään salausavaimen saamiseksi kahden päätelaitteen väliseen kommunikointiin, ja

kuvio 10 havainnollistaa järjestelmän erästä vaihtoehtoista toteutustapaa.

Keksinnön yksityiskohtainen kuvaus

Seuraavassa keksintöä kuvataan viitaten verkkoympäristöön, jossa tilaajien liikkuvuutta tuetaan Mobile IP -protokollan (jatkossa MIP) avulla. MIP on olemassa olevan IP:n versio, joka tukee päätelaitteen liikkuvuutta. (MIP-periaatetta kuvataan esim. RFC 2002:ssa, October 1996 tai artikkelissa Upkar Varshney, *Supporting Mobility with Wireless ATM*, Internet Watch, January 1997.)

MIP perustuu siihen, että kullakin liikkuvalla tietokoneella tai solmulla (mobile host, mobile node) on sille osoitettu agentti ("kotiagentti", home agent), joka välittää paketit liikkuvan solmun sen hetkiseen sijaintipaikkaan. Kun liikkuva solmu liikkuu aliverkosta toiseen, se rekisteröityy kyseistä aliverkkoa palvelevalle agentille ("vierailuagentti", foreign agent). Viimemainittu suorittaa tarkistuksia liikkuvan solmun kotiagentin kanssa, rekisteröi liikkuvan solmun ja lähettää sille rekisteröinti-informaation. Liikkuvalle solmulle osoitetut paketit lähetetään liikkuvan solmun alkuperäiseen sijaintipaikkaan (kotiagentille), josta

ne välitetään edelleen sen hetkiselle vierailuagentille, joka lähettää ne edelleen liikkuvalle solmulle.

Kuviossa 1 on esitetty keksinnön mukaisen menetelmän tyypillistä toimintaympäristöä. Järjestelmän ytimen muodostaa turvapalvelin SS, joka on toisaalta kytketty Internetiin ja toisaalta proxy-palvelimeen HP, jolla on pääsy erilliseen matkaviestinverkkoon MN, joka on tässä esimerkissä GSM-verkko. Proxy-palvelin muodostaa verkkoelementin, joka välittää (myöhemmin kuvattavalla tavalla) liikennettä turvapalvelimen ja matkaviestinverkkojen kotirekisterien HLR välillä, jotka viimemainitut sijaitsevat tilaajien kotiverkoissa. Käytännössä sekä proxy- että turvapalvelin ovat verkko-operaattorin tiloissa, esim. samassa huoneessa, joten vaikka turvapalvelimen ja proxy-palvelimen välillä onkin IP-yhteys, se on turvattu yhteys. Koska GSM-verkko on sinänsä tunnettu, eikä keksintö edellytä muutoksia siihen, ei sitä kuvata tässä yhteydessä tarkemmin.

Järjestelmän alueella liikkuvilla käyttäjillä on käytössään kannettavia tietokoneita, PDA-laitteita, älypuhelimia tai muita vastaavia päätelaitteita. Kuviossa on viitemerkillä ASIAKAS (client) havainnollistettu vain yhtä päätelaitetta TE1. Asiakkaalla tarkoitetaan tässä yhteydessä yleisesti oliota, joka käyttää verkon tarjoamia palveluja, joita verkon palvelimet suorittavat. Usein asiakkaalla tarkoitetaan ohjelmaa, joka ottaa verkon käyttäjän puolesta yhteyttä palvelimeen.

Kuvioon on merkitty kaksi aliverkkoa, jotka voivat käytännössä olla esim. Ethernet-lähiverkkoja, joissa siirretään TCP/IP-paketteja: kyseisen käyttäjän kotiverkko HN sekä vierailuverkko FN, johon päätelaitteen TE1 oletetaan olevan yhteydessä. Nämä aliverkot ovat kumpikin yhdyskäytäväkoneen GW (reitittimen) avulla yhteydessä Internetiin. Kotiverkossa on kyseisen liikkuvan tietokoneen kotiagentti HA ja vierailuverkossa vastaavasti vierailuagentti FA. Liitynnät aliverkkoihin tapahtuvat liittymäpisteiden (access point) AP kautta, esim. langattomasti, kuten kuviossa esitetään.

Päätelaitteet muodostuvat kahdesta osasta samaan tapaan kuin tavanomainen GSM-puhelin: varsinaisesta tilaajalaitteesta, esim. kannettavasta tietokoneesta (ohjelmistoineen) ja SIM-kortista (Subscriber Identity Module), jolloin tilaajalaitteesta tulee verkon kannalta toimiva päätelaite vasta kun SIM-kortti on työnnetty siihen. SIM-kortti on tässä esimerkkitapauksessa GSM-verkossa käytettävä tilaajan tunnistusyksikkö. Päätelaitteella voi olla pääsy vain IP-verkkoon tai se voi olla ns. dual mode -laite, jolla on pääsy sekä

IP-verkkoon että GSM-verkkoon. Liityntä IP-verkkoon tapahtuu esim. päätelaitteessa olevan LAN-kortin avulla ja GSM-verkkoon GSM-kortin avulla, joka on käytännössä riisuttu puhelin, joka on sijoitettu esim. tietokoneen PCMCIA-korttipaikkaan.

Keksinnön edullisessa toteutustavassa turvapalvelimen yhteydessä on myös sinänsä tunnettu Kerberos-palvelin KS, jonka avulla toteutetaan salatut yhteydet jäljempänä kuvattavalla tavalla. Turvapalvelin ja Kerberos-palvelin voivat olla fyysisesti samalla koneella.

Jotta turvapalvelin tietäisi, koska käyttäjä tulee IP-verkkoon tai poistuu siitä, luodaan turvapalvelimen ja kotiagentin välille kanava kuviossa 2 esitetyllä tavalla. MIP-protokollan mukaisesti vierailuagentti FA lähettää omaan aliverkkoonsa jatkuvasti broadcast-sanomia, joita kutsutaan nimellä "agent advertisement" ja joita on kuviossa merkitty viitemerkillä AA. Kun päätelaite kytkeytyy kyseiseen aliverkkoon, se vastaanottaa näitä sanomia ja päättelee niiden perusteella, onko se omassa kotiverkossaan vai jossakin muussa verkossa. Jos päätelaite huomaa, että se on kotiverkossaan, se toimii ilman liikkuvuuteen liittyviä palveluja (mobility services). Muussa tapauksessa päätelaite saa c/o-osoitteen (care-of address) ko. vieraaseen verkkoon. Tämä osoite on verkon sen pisteen osoite, johon päätelaite on väliaikaisesti kytkeytyneenä. Tämä osoite muodostaa samalla ko. päätelaitteelle johtavan tunnelin (tunnel) päätepisteen (termination point). Päätelaite saa osoitteen tyypillisesti em. broadcast-sanomista, joita vierailuagentti lähettää. Tämän jälkeen päätelaite lähettää omalle kotiagentilleen rekisteröintipyyntösanoman RR (Registration Request) vierailuagentin FA kautta. Sanoma sisältää mm. sen c/o-osoitteen, jonka päätelaite on juuri saanut. Vastaanottamansa pyyntösanoman perusteella kotiagentti päivittää kyseisen päätelaitteen sijaintitiedon tietokantaansa ja lähettää päätelaitteelle vierailuagentin kautta rekisteröintivastauksen (Registration Reply) R_Reply. Vastaussanomassa on kaikki tarpeelliset tiedot siitä, miten (millä ehdoilla) kotiagentti on hyväksynyt rekisteröintipyynnön.

Kaikki edellä kuvatut, päätelaitteen, vierailuagentin ja kotiagentin väliset sanomat ovat normaaleja MIP-protokollan mukaisia sanomia. Liikkuva solmu voi rekisteröityä myös suoraan kotiagentille. Em. RFC:ssä on kuvattu ne säännöt, jotka määräävät sen, rekisteröityykö liikkuva solmu kotiagentille suoraan vai vierailuagentin kautta. Jos liikkuva solmu saa c/o-osoitteen edellä kuvatulla tavalla, on rekisteröinti tehtävä aina vierailuagentin kautta. MIP-protokollan mukaan rekisteröinnin yhteydessä suoritetaan myös autentikointi,

jonka tarkoituksena on vähentää virheiden esiintymistä rekisteröitymisen yhteydessä. Rekisteröinti perustuu rekisteröintisanomasta (rekisteröintipyynnöstä tai -vastauksesta) laskettuun tarkistusarvoon ja rekisteröinti on tehtävä vain liikkuvan solmun ja sen kotiagentin välillä, joilla on yhteisesti jaettu kiinteä avain (joka on etukäteen sovittu). Vierailuagentti ei näin ollen välttämättä pysty autentikoimaan liikkuvaa solmua. Tämä ongelma korostuu, jos järjestelmässä pyritään mahdollisimman laajaan maantieteelliseen kattavuuteen.

Keksinnön mukaisesti kotiagenttiin on lisätty toiminne, jonka mukaan kotiagentti lähettää turvapalvelimelle tiedon verkkoon kytkeytyvästä päätelaitteesta sen jälkeen, kun rekisteröintipyyntösanoma on tullut vierailuagentilta. Tätä sanomaa on kuviossa merkitty viitemerkillä MOB_ATTACH. Vastaavasti kotiagentti lähettää turvapalvelimelle tiedon verkosta poistuneesta päätelaitteesta sen jälkeen, kun päätelaite on kytkeytynyt irti verkosta (päätelaite kytkeytynyt irti verkosta tai sille annetun osoitteen elinaika on umpeutunut). Tätä sanomaa on kuviossa merkitty viitemerkillä MOB_DETACH. Kumpaankin sanomatyyppiin turvapalvelin lähettää kuittaussanoman (MOB_ACK). Sanomat MOB_ATTACH ja MOB_DETACH vastaavat käyttötarkoitukseltaan GSM-verkossa käytettäviä IMSI attach/detach -proseduureja.

Kotiagentti monitoroi turvapalvelimelta tulevia vastauksia ja lähettää sanomat uudelleen (samoilla parametreillä), jos turvapalvelimelta ei tule kuittaussanomaa ennalta määrätyn pituisen ajan, esim. 30 sekunnin, kuluessa.

Kuviossa 3 on havainnollistettu sanomien MOB_ATTACH, MOB_DETACH ja MOB_ACK rakennetta. Sanomissa on tyyppikenttä 31, joka identifioi sanoman tyypin, numerokenttä 32, joka sisältää istunnon identifioivan satunnais- tai järjestysnumeron ja osoitekenttä 33, joka sisältää asiakkaan IP-osoitteen. Viimemainittua kenttää ei ole kuittaussanomassa. Sanomat lähetetään IP-tietosähkeiden hyötykuormalle varatuissa kentissä.

Kun siis päätelaite on kytkeytynyt verkkoon, turvapalvelin saa siis kotiagentilta tiedon ko. päätelaitteen IP-osoitteesta. Tämän jälkeen seuraa asiakkaan autentikointi, jota kuvataan seuraavassa viitaten kuvioon 4. Autentikointia varten turvapalvelin kysyy ensin asiakkaalta tilaajatunnusta IMSI (International Mobile Subscriber Identity), joka on talletettu SIM-kortille (sanoma AUTH_ID_REQ). Tähän asiakas vastaa antamalla vastaussanomassa AUTH_ID_RSP tilaajatunnuksensa IMSI (joka on GSM-spesifikaatioiden mukainen 9 tavun pituinen tunniste). Kysely kulkee kotiagentin kautta em. tunnelin päätepisteeseen, mutta vastaus tulee päätelaitteelta suoraan turva-

palvelimelle.

Jos asiakkaan IP-osoite ei vaihdu usein, on edullisempaa tallettaa turvapalvelimelle IP-osoitteita vastaavat IMSI-tunnisteet, jolloin tunnisteita ei tarvitse turhaan siirtää verkossa. Edellä mainitut sanomat eivät siten ole välttämättömiä.

Kun päätelaite on ilmoittanut IMSI-tunnisteensa tai kun turvapalvelin on hakenut sen tietokannastaan, turvapalvelin käynnistää varsinaisen autentikoinnin. Jotta päätelaitteen SIM-kortti voitaisiin autentikoida, turvapalvelimelta on oltava yhteys tilaajan oman GSM-verkon kotirekisterin HLR yhteydessä olevaan tunnistuskeskukseen AuC (Authentication Center). Tämä toteutetaan proxy-palvelimella HP, joka toimii yhdistävänä verkkoelementtinä IP-verkon ja GSM-verkon, tarkemmin sanottuna IP-verkon ja GSM-verkon käyttämän SS7-merkinantoverkon välillä. Autentikoinnissa tarvittava GSM-verkon palvelu on MAP_SEND_AUTHENTICATION_INFO (GSM 9.02, v. 4.8.0). Tämä palvelu toteutetaan proxy-palvelimen HP avulla, joka voidaan sijoittaa paikallisen GSM-operaattorin tiloihin. Turvapalvelin lähettää proxy-palvelimelle autentikointipyyntösanoman SEC_INFO_REQ, joka sisältää yhteysistuntotunnisteen ja tilaajatunnuksen IMSI. Proxy-palvelin lähettää puolestaan tunnistuskeskukselle AuC MAP-protokollan (Mobile Application Part) mukaisen kyselysanoman, jolla pyydetään tunnistuskolmikkoa (authentication triplet) ja joka lähetetään normaalisti VLR:n ja HLR:n välillä. Vasteena tälle kyselysanomalle HLR palauttaa proxy-palvelimelle tavanomaisen tunnistuskolmikon, joka sisältää haasteen (RAND), vasteen SRES (Signed Response) ja avaimen Kc (GSM-verkossa käytettävä yhteyskohtainen salausavain). Proxy-palvelin välittää kolmikon edelleen turvapalvelimelle sanomassa SEC_INFO_RSP. Turvapalvelin tallettaa kolmikon ja lähettää (sanoma AUTH_CHALLENGE_REQ) haasteen edelleen päätelaitteen SIM-kortille, joka generoi sen perusteella vasteen (SRES) ja avaimen Kc. Päätelaite tallettaa avaimen ja lähettää (sanoma AUTH_CHALLENGE_RSP) vasteen (SRES) takaisin turvapalvelimelle.

Päätelaitteessa on edullista olla tietokanta, johon haasteet talletetaan. Tällä tavalla pystytään varmistautumaan siitä, että yhtä haastetta käytetään vain kerran. Tällä tavalla pystytään estämään se, ettei kukaan pysty esiintymään turvapalvelimena nappaamalla verkosta (salaamattoman) haasteen ja vasteen ja selvittämällä niiden perusteella avaimen Kc. Jos sama haaste tulee uudelleen, ei ko. haasteeseen vastata. Turvapalvelin voi myös suodattaa

sellaiset haasteet, jotka on jo käytetty ja tarvittaessa pyytää uutta tunnistuskolmikkoa GSM-verkosta, jotta päätelaitteelle ei turhaan lähetetä jo käytettyä haastetta.

Proxy-palvelin HP toimii järjestelmässä virtuaalisena vierailijarekisterinä VLR, koska se näkyy, ainakin tunnistuskolmikkokyselyjen osalta, kotirekisteristä päin samanlaiselta verkkoelementiltä kuin GSM-verkon aidot vierailijarekisterit. Proxy-palvelin toimii myös suodattimena, joka sallii vain tunnistuskolmikkokyselyjen pääsyn GSM-järjestelmän signalointiverkkoon. Proxy-palvelin ei myöskään häiritse muita GSM-verkon puolella kotirekisteriltä tehtäviä kyselyjä.

Kuviossa 5 on havainnollistettu kuviossa 4 esitettyjen sanomien yleistä rakennetta. Sanomissa on tyyppikenttä 51, joka identifioi sanoman tyypin, numerokenttä 52, joka sisältää istunnon identifioivan satunnais- tai järjestysnumeron ja hyötykuormakenttä 53, jonka pituus vaihtelee sen mukaan, mikä sanoma on kysymyksessä. Turvapalvelimen ja päätelaitteen välisissä sanomissa kaksi ensimmäistä kenttää ovat kaikissa sanomissa, mutta hyötykuormakenttää ei ole sanomassa AUTH_ID_REQ. Sanomassa AUTH_ID_RSP hyötykuormakenttä on 9 tavun pituinen (IMSIn pituus 1+8 tavua), sanomassa AUTH_CHALLENGE_REQ 16 tavun pituinen (RANDin pituus 16 tavua) ja sanomassa AUTH_CHALLENGE_RSP 4 tavun pituinen (SRES on 4 tavun pituinen). Turvapalvelimen ja proxy-palvelimen välisissä sanomissa hyötykuormakenttä on 9 tavun pituinen (IMSI) sanoman SEC_INFO_REQ tapauksessa ja n×28 tavun pituinen sanoman SEC_INFO_RSP tapauksessa (kolmikossa on yhteensä 28 tavua ja verkkoelementit on yleensä konfiguroitu niin, että ne lähettävät 1...3 tilaajakohtaista kolmikkoa kerrallaan). Kuten aiemmin todettiin, proxy-palvelimen ja kotirekisterin HLR välillä käytetään tavanomaista GSM-verkon merkinantoa.

Turvapalvelin vertaa päätelaitteelta vastaanottamaansa vastetta kolmikossa tulleeseen vasteeseen ja mikäli vertailussa havaitaan, että vasteet ovat samat, autentikointi on onnistunut.

Vasteena onnistuneelle autentikoinnille turvapalvelin käynnistää rekisteröinnin Kerberos-palvelimelle. Kerberos-palvelimella tarkoitetaan tässä yhteydessä prosessia, joka tarjoaa Kerberos-palvelua. Kerberos-palvelin sijaitsee edullisesti turvapalvelimen yhteydessä, kuten kuviossa 1 esitetään.

Kerberos on järjestelmä, joka on tarkoitettu verkon käyttäjien ja palvelujen autentikointiin. Se on luotettu (trusted) palvelu siinä mielessä, että

kukin sen asiakkaista luottaa siihen, että järjestelmän arvio sen kaikista muista asiakkaista on oikea. Koska Kerberos-järjestelmä on sinänsä tunnettu, eikä sen toimintaa muuteta mitenkään, ei sitä kuvata tässä yhteydessä yksityiskohtaisesti. Järjestelmää kuvataan esim. dokumentissa Steiner, Neuman, Schiller: Kerberos: An Authentication Service for Open Network Systems, January 12, 1988, josta kiinnostunut lukija löytää halutessaan taustainformaatiota. Seuraavassa kuvauksessa käytetään samoja merkintätapoja kuin em. dokumentissa. Kuvaus perustuu Kerberoksen versioon 4.

c → asiakas (client),
s → palvelin
c-addr → asiakkaan verkko-osoite
tgs → pääsylipunantopalvelin
K_x → x:n henkilökohtainen avain
$K_{x,y}$ → istuntoavain x:lle ja y:lle
$\{abc\}K_x$ → abc salattuna x:n henkilökohtaisella avaimella
Tx,y → x:n pääsylippu y:n käyttämiseksi.

Kuviossa 6 on havainnollistettu Kerberos- ja autentikointisovellusten olioita. Kuviossa on oletettu, että järjestelmällä on kaksi asiakasta, A ja B. Kumpikin asiakas voi olla päätelaite, jonka turvapalvelin on autentikoinut edellä kuvatulla tavalla, kun ne ovat kytkeytyneet IP-verkkoon tai toinen voi olla "kiinteästi" autentikoitu asiakas, esim. palvelin. Kerberos-sovellus koostuu kahdesta osasta: asiakasohjelmasta KC, joka sijaitsee päätelaitteella ja palvelinohjelmasta KS, joka sijaitsee turvapalvelimella. Palvelinohjelmaan kuuluu myös pääsylipunantopalvelin TGS (ticket granting server). Vastaavasti autentikointisovellus koostuu kahdesta osasta: asiakasohjelmasta AC, joka sijaitsee päätelaitteella ja palvelinohjelmasta AS, joka sijaitsee turvapalvelimella. Kommunikointi tapahtuu IP/MIP/IP-SEC-pinojen avulla, joita kuvataan tarkemmin jäljempänä.

Seuraavassa kuvataan, kuinka Kerberos-protokollaa käytetään luomaan yhteyskohtainen avain päätelaitteiden A ja B välille.

Kun turvapalvelin on havainnut autentikoinnin onnistuneen, se käynnistää Kerberos-asiakkaan rekisteröinnin Kerberos-palvelimelle. Käytännössä tämä tapahtuu siten, että turvapalvelimen autentikointilohko AS rekisteröi tunnistuskolmikossa tulleen avaimen Kc (a) asiakkaan salasanana ja (b) salasanana palveluun, joka muodostetaan asiakkaan IP-osoitteelle tai tilaajatunnukselle IMSI. Palvelulle annetaan jokin ennalta määrätty nimi.

Tämän jälkeen asiakas voi hakea pääsylipun (ticket) pääsylipunantopalvelinta varten käyttäen avainta Kc. Tätä sanomanvaihtoa on esitetty kuviossa 7. Sen jälkeen, kun asiakas on saanut avaimen Kc, se lähettää turvapalvelimelle (Kerberos-palvelimelle) sanoman, jolla pyydetään Kerberos-järjestelmältä aloituspääsylippua (initial ticket). Avaimen saamisen ja sanoman lähettämisen välillä voi olla lyhyt ennalta määrätty viive, jotta turvapalvelin ehtii ensin suorittaa rekisteröinnin Kerberos-palvelimelle. Viiveen jälkeen päätelaite lähettää turvapalvelimelle Kerberos-protokollan mukaisen pyynnön, joka sisältää aina asiakkaan identiteetin (IMSIn tai IP-osoitteen) ja tietyn erikoispalvelun, pääsylipunantopalvelun (ticket granting service) nimen tgs. Saatuaan tämän kyselyn Kerberos-palvelin tarkistaa, että se tuntee asiakkaan. Jos näin on, se generoi satunnaisen yhteyskohtaisen avaimen $K_{c,tgs}$, jota tullaan myöhemmin käyttämään asiakkaan ja pääsylipunanto-palvelimen välisessä tiedonsiirrossa. Tämän jälkeen Kerberos-palvelin generoi pääsylipun $T_{c,tgs}$, jolla asiakas voi käyttää pääsylipunanto-palvelua. Tämä pääsylippu sisältää asiakkaan nimen, pääsylipunanto-palvelimen nimen, sen hetkisen kellonajan, pääsylipun elinajan, asiakkaan IP-osoitteen ja juuri edellä generoidun yhteyskohtaisen avaimen. Käyttäen edellä esitettyjä merkintätapoja pääsylipun sisältö voidaan esittää seuraavasti $T_{c,tgs}=\{c, tgs, timestamp, lifetime, c\text{-}addr, K_{c,tgs}\}$. Tämä pääsylippu salataan avaimella K_{tgs}, jonka vain pääsylipunanto-palvelin ja Kerberos-palvelin tietävät. Tämän jälkeen Kerberos-palvelin lähettää asiakkaalle vasteena paketin, joka sisältää salatun pääsylipun ja yhteyskohtaisen avaimen $K_{c,tgs}$ kopion. Vaste on salattu asiakkaan omalla avaimella Kc. Päätelaite tallettaa pääsylipun ja istuntoavaimen tulevaa käyttöä varten.

Kun päätelaite on tallettanut pääsylipun ja istuntoavaimen, sillä on, pääsylipun elinaikana, pääsy pääsylipunanto-palveluun ja se on valmis olemaan yhteydessä kolmannen osapuolen kanssa.

Kuviossa 8 on havainnollistettu päätelaitteen niitä toiminnallisia lohkoja, jotka ovat oleellisia keksinnön kannalta. Päätelaite on yhteydessä verkkoon IP/MIP/IP-SEC-protokollapinon kautta. IP/MIP/IP-SEC on sellainen tunnettu TCP/IP-pino, jonka sisään on rakennettu mobile IP - ominaisuudet ja salaustoiminnot. Ylhäältä päin tämä pino näyttää aivan tavalliselta IP-pinolta, mutta alhaalta (verkon puolelta) ko. pino lähettää salattua informaatiota tietyn turvapolitiikan (security policy) mukaisesti. Tämän turvapolitiikan määrää erillinen turvapolitiikkalohko SPB, joka ohjaa IP/MIP/IP-SEC-pinoa kertomalla pinolle, mihin muihin verkon olioihin on lähetettävä salattua informaatiota.

Nämä oliot on yleensä määritelty turvapolitiikkalohkossa päätelaitteen IP-osoitteen ja porttinumeron avulla. Määrittely voidaan tehdä vielä hienojakoisemmaksi määrittelemällä lisäksi ne käyttäjätunnukset, joille salausta suoritetaan. Turvapolitiikkalohko on käytännössä rakennettu IP/MIP/IP-SEC-pinon sisään, mutta toiminnallisessa mielessä se on oma lohkonsa.

Turvapolitiikkalohkon lisäksi päätelaitteessa on avaimienhallintalohko KM, joka huolehtii avaimien hallinnasta. Avaimienhallintalohkon yhteydessä on tietokanta, jossa on kaikki päätelaitteen käyttämät salausavaimet. Avaimienhallintalohko voidaan toteuttaa esim. tunnetun PF_KEY-avaimienhallinta-APIn (API=Application Programming Interface) avulla. PF_KEY on geneerinen sovellusohjelmaliitäntä, jota voidaan käyttää IP-kerroksen turvapalvelujen lisäksi myös verkon muihin turvapalveluihin. Tämä API määrittelee socket-protokollaperheen, jota avaimienhallintasovellukset käyttävät kommunikoidakseen käyttöjärjestelmän avaimienhallintaan liittyvien osien kanssa. Koska keksintö ei liity tunnettuun PF_KEY-protokollaan, ei sitä kuvata tässä yhteydessä tarkemmin. Protokollaa kuvataan dokumentissa McDonald, Metz, Phan: PF_KEY Management API, version 2, 21 April, 1997, josta aiheesta kiinnostunut lukija löytää halutessaan taustainformaatiota.

Avaimienhallintalohkossa KM on omat määrittelynsä sille, miten ja millä avaimella salaus toteutetaan kuhunkin verkko-osoitteeseen. Tämä määrittely voi olla tehty esim. siten, että IP-osoite- ja porttikohtaisesti kerrotaan se protokolla ja se avain, jota on käytettävä, kun ollaan yhteydessä ko. porttiin.

Kun ulospäin lähetettävä paketti tulee IP/MIP/IP-SEC-pinoon, pino lukee paketin kohdeosoitteen ja kysyy turvapolitiikkalohkolta SPB, mikä on salauspolitiikka ko. osoitteella varustetun paketin suhteen. Turvapolitiikkalohko kertoo vasteena IP/MIP/IP-SEC-pinolle, tehdäänkö salaus ja jos tehdään, millä menetelmällä salaus suoritetaan. Nämä tiedot välitetään avaimienhallintalohkolle KM.

Alkuvaiheessa käyttäjä on määritellyt turvapolitiikkalohkolle ne yhteydet, joilla on käytettävä salausta. Jos turvapolitiikkalohko ilmoittaa, että salausta on käytettävä ja jos avaimienhallintalohko huomaa, että sitä päätelaitetta varten, jonka kanssa halutaan olla yhteydessä, ei ole vielä avainta, avaimienhallintalohko lähettää avainpyynnön Kerberos-asiakkaalle KC, joka kysyy turvapalvelimen pääsylipunantopalvelulta palvelinpääsylippua ko. päätelaitetta varten. Tätä merkinantoa on havainnollistettu kuviossa 9. Päätelaite (Kerberos-asiakas) lähettää pääsylipunantopalvelimelle Kerberos-protokollan

mukaisen pyynnön, joka sisältää sen palvelimen nimen (s, esim. päätelaite B), jolle pääsylippu halutaan, pääsylipunantopalvelimen omalla avaimella K_{tgs} salatun pääsylipun $T_{c,tgs}$ pääsylipunantopalveluun pääsyä varten ja autentikaattorin (authenticator) Ac, joka on salattu yhteyskohtaisella avaimella $K_{c,tgs}$. Autentikaattori on tietorakenne, joka sisältää asiakkaan nimen ja IP-osoitteen sekä sen hetkisen ajan. Käytettyä merkintätapaa noudattaen Ac = {c, c-addr, timestamp}.

Pääsylipunantopalvelin tarkistaa autentikaattorin tiedot ja pääsylipun $T_{c,tgs}$. Jos pääsylippu on kelvollinen, pääsylipunanto-palvelin generoi uuden satunnaisen istuntoavaimen $K_{c,s}$, jota asiakas voi käyttää haluamansa kolmannen osapuolen kanssa. Sen jälkeen pääsylipunantopalvelin muodostaa uuden pääsylipun $T_{c,s}$ mainittua kolmatta osapuolta varten, salaa pääsylipun mainitun kolmannen osapuolen omalla avaimella K_s, joka on sama kuin ko. tilaajan edellä kuvattu avain Kc, ja lähettää salatun pääsylipun yhdessä istuntoavaimen kanssa päätelaitteelle. Koko vastaus salataan avaimella $K_{c,tgs}$.

Saatuaan vastaussanoman päätelaite purkaa paketin, lähettää ensimmäisen osan $\{T_{c,s}\}K_s$ kolmannelle osapuolelle (päätelaitteelle B) ja tallettaa uuden istuntoavaimen $K_{c,s}$ avaintietokantaan. Kolmannen osapuolen päätelaite saa juuri generoidun istuntoavaimen $K_{c,s}$ pääsylipusta purkamalla pääsylipun ensin omalla avaimellaan Kc. Tämän jälkeen uusi istuntoavain on molempien päätelaitteiden käytössä ja salattu tiedonsiirto voi alkaa.

Kun Kerberos-asiakas on aloittanut toimintansa (kun asiakas on rekisteröity Kerberos-palvelimelle), sen täytyy informoida IP/MIP/IP-SEC-kerrosta siitä, että se pystyy palvelemaan istuntoavainpyyntöjä. Tämä tapahtuu PF_KEY-protokollaa käyttäen siten, että Kerberos-asiakas avaa erityisen socket-osoitteen käyttöjärjestelmän ytimeen (kernel) ja rekisteröityy ytimeen SADB_REGISTER-sanomalla. Tämän jälkeen PF_KEY-protokolla lähettää SADB_ACQUIRE-sanoman joka kerta, kun avainta tarvitaan johonkin ulospäin lähtevään liitäntään. Saadessaan tämän sanoman Kerberos-asiakas toimii edellä kuvatulla tavalla eli lähettää pyynnön pääsylipunantopalvelimelle, lähettää saamastaan vasteesta vastapuolelle tarkoitetun osan yhteyden vastakkaiseen päähän ja välittää saamansa istuntoavaimen avaimienhallintalohkolle. Lisäksi Kerberos-asiakas kuuntelee tiettyä socket-osoitetta havaitakseen verkon muilta olioilta mahdollisesti tulevat pääsyliput. Vastaanotettuaan tällaisen pääsylippupaketin se kuittaa vastaanottaneensa paketin, purkaa paketin ja välittää tarpeelliset avaimet avaimienhallintajärjestelmälle, jolloin näitä

avaimia voidaan käyttää oltaessa yhteydessä kyseiseen vastekerrokseen (peer).

Kun päätelaite poistuu verkosta (sanoma MOB_DETACH), turvapalvelin poistaa molemmat rekisteröinnit Kerberos-palvelimelta.

Käytännössä on päätelaitteilla ja turvapalvelimella oltava määrätyt porttinumerot auki salaamatonta tiedonsiirtoa varten. Tällaisia portteja ovat portti, jonka kautta lähetetään päätelaitteen ja palvelimen väliset autentikointisanomat (kuvio 4), portti, jonka kautta välitetään tiketit Kerberos-asiakkaille ja portti, jonka kautta välitetään pääsylippupyynnöt.

Tunnistuskolmikko voidaan hakea eri tavoilla. Pienimuotoisessa toteutuksessa voitaisiin toimia siten, että käytetään virtuaalista "HLR-tietokantaa", johon talletetaan valmiiksi sopivaksi katsottava määrä tunnistuskolmikkoja. Esim. 10000 kolmikkoa jokaiselta käyttäjältä vaatisi 280 kilotavua muistia käyttäjää kohti. Näin ollen esim. 6 GB levylle saataisiin yli 21000 käyttäjän tunnistuskolmikot. Tunnistuskolmikot voidaan ladata etukäteen silloin, kun käyttäjä saa palvelun, jättämällä SIM-kortti muutamaksi tunniksi älykortinlukijaan, joka syöttää kortille haasteita. Saaduista vasteista muodostetut tunnistuskolmikot talletetaan tietokantaan kortin tietoja käyttäen. Tämä tapa toimii myös kaikilla SIM-korteilla operaattoreista riippumatta. Tietokanta voi olla esim. turvapalvelimen yhteydessä. Tunnistuskolmikko(j)a ei siis välttämättä tarvitse hakea matkaviestinverkosta, vaan tilaajakohtaisia tunnistuskolmikoita voidaan tallettaa etukäteen turvapalvelimen yhteydessä olevaan tietokantaan DB (vrt. kuvio 1). Proxy-palvelimia ei siis välttämättä tarvita lainkaan. Osalle tilaajia voi myös olla valmiita tunnistuskolmikkoja tietokannassa ja osalle ne voidaan hakea reaaliaikaisesti matkaviestinjärjestelmästä. Tunnistuskolmikkoja voidaan myös hakea etukäteen matkaviestinjärjestelmästä tietokantaan.

Periaatteessa voidaan myös kopioida jokaisen käyttäjän SIM-kortti ja käyttää kopiota turvapalvelimen yhteydessä käyttäjän autentikoimiseksi (jolloin matkaviestinverkosta ei tehdä kyselyä).

Nämä kaksi edellä kuvattua menettelyä mahdollistavat sen, että käytetyt SIM-kortit voivat olla vain tähän tarkoitukseen dedikoituja kortteja, eivätkä ne välttämättä liity matkaviestinverkon tilaajaan.

Tarvittava autentikointitieto voidaan saada GSM-verkosta myös esim. matkaviestinkeskuksen MSC (Mobile Switching Centre) ja tukiasemaohjaimen BSC (Base Station Controller) väliseltä yhteydeltä. Proxy-palvelimen ei siten välttämättä tarvitse emuloida vierailijarekisteriä VLR, kuten edellä esitettiin,

vaan se voi toimia myös GSM-verkon tukiasemaohjaimen kaltaisena verkkoelementtinä. Tällaista vaihtoehtoa on havainnollistettu kuviossa 10, jossa kyseistä verkkoelementtiä on merkitty viitemerkillä BP. Tässä tapauksessa proxy-palvelin on siis virtuaalinen tukiasemaohjain, joka on kytketty matkaviestinkeskukseen MSC (Mobile Switching Centre) samalla tavoin kuin GSM-verkon normaalit tukiasemaohjaimet BSC (Base Station Controller). Matkaviestinkeskukselta päin katsottuna proxy-palvelin näyttää tavanomaiselta tukiasemaohjaimelta ainakin autentikointiin liittyvän merkinannon osalta.

Ongelmana tässä toisessa vaihtoehdossa on kuitenkin se, että se edellyttää huomattavasti monimutkaisempaa merkinantoa proxy-palvelimen ja GSM-verkon välillä kuin ensimmäinen vaihtoehto (kuvio 1). Toisen vaihtoehdon mukaisen autentikoinnin seurauksena käyttäjä siirtyy lisäksi GSM-järjestelmässä tukiasemaohjainta emuloivan proxy-palvelimen BP alueelle, joka ei kuitenkaan ole oikea tukiasemaohjain siinä mielessä, että se pystyisi välittämään myös puheluja. Näin ollen tätä ratkaisua voidaan käyttää vain datapalvelujen yhteydessä, eikä päätelaite voi olla em. dual mode -laite.

Vaikka keksintöä on edellä kuvattu viitaten MIP-enabloituun verkkoon, keksinnön mukainen ratkaisu ei ole sidottu tähän protokollaan. Jos käytettävä protokolla on IPv6, ei verkossa ole varsinaisia agentteja. Tällöin joudutaan tieto siitä, milloin käyttäjä on verkossa hakemaan käyttäjän kotiverkon reitittimen reititystauluista. Käytännössä tämä tarkoittaa sitä, että verkossa on oltava erillinen "paikannusagentti", joka reititintä monitoroimalla tai "pingaamalla" huomaa käyttäjän tulleen verkkoon ja käynnistää sen seurauksena autentikoinnin lähettämällä turvapalvelimelle ilmoituksen (MOB_ATTACH) uudesta käyttäjästä. Luultavaa kuitenkin on, että reititinvalmistajat suunnittelevat protokollan, josta ilmenee, milloin käyttäjä on verkossa.

Vaikka keksintöä on edellä selostettu viitaten oheisten piirustusten mukaisiin esimerkkeihin, on selvää, ettei keksintö ole rajoittunut siihen, vaan sitä voidaan muunnella oheisissa patenttivaatimuksissa esitetyn keksinnöllisen ajatuksen puitteissa. Autentikointia ei välttämättä tarvitse suorittaa salatun yhteyden muodostamiseksi käyttäjien välillä, vaan onnistuneen autentikoinnin seurauksena voidaan suorittaa esim. rekisteröinti postipalvelimelle ennen sähköpostiviestien siirtoa käyttäjän koneelle. Tällä tavoin saadaan varmempi autentikointi kuin nykyisissä salasanoihin perustuvissa menetelmissä. Liittymäpisteiden yhteydessä voi lisäksi olla paikallisia palvelimia, jotka toimivat proxy-palvelimina varsinaiselle turvapalvelimelle tai järjestelmässä voi olla

useampi kuin yksi turvapalvelin. Kerberos-järjestelmän tilalla voidaan käyttää myös esim. julkisten avainten avainhallintaa, joka perustuu x.500-tietokantaan ja x.509 sertifikaatteihin.

Patenttivaatimukset

1. Autentikointimenetelmä tietoliikenneverkkoja, erityisesti IP-verkkoja varten, jonka menetelmän mukaisesti todennetaan verkkoon kytkeytyneen tilaajan identiteetti,

t u n n e t t u siitä, että

- verkon päätelaitteessa (TE1) käytetään oleellisesti samanlaista tilaajan tunnistusyksikköä (SIM) kuin tunnetussa matkaviestinjärjestelmässä (MN), joka tunnistusyksikkö on sellainen, että sille syötteenä annetusta haasteesta saadaan tuloksena vaste,

- verkossa käytetään lisäksi erityistä turvapalvelinta (SS) siten, että päätelaitteen kytkeytyessä verkkoon turvapalvelimelle lähetetään ilmoitus uudesta käyttäjästä,

- haetaan mainittua uutta käyttäjää vastaavan tilaajan autentikointi-informaatio mainitusta matkaviestinjärjestelmästä mainittuun verkkoon, joka autentikointi-informaatio sisältää ainakin haasteen ja vasteen, ja

- autentikointi suoritetaan matkaviestinjärjestelmästä saadun autentikointi-informaation perusteella lähettämällä verkon kautta mainittu haaste päätelaitteelle, generoimalla päätelaitteen tunnistusyksikössä haasteesta vaste ja vertaamalla vastetta matkaviestinjärjestelmästä saatuun vasteeseen.

2. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tilaajan autentikointi-informaation haku matkaviestinjärjestelmästä käynnistetään turvapalvelimelta (SS) vasteena mainitulle ilmoitukselle.

3. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että vasteena onnistuneelle autentikoinnille suoritetaan tilaajan rekisteröinti erillisen avainten hallintajärjestelmän asiakkaaksi.

4. Patenttivaatimuksen 3 mukainen menetelmä IP-verkkoja varten, t u n n e t t u siitä, että avainten hallintajärjestelmänä käytetään tunnettua Kerberos-järjestelmää.

5. Patenttivaatimuksen 4 mukainen menetelmä, t u n n e t t u siitä, että matkaviestinjärjestelmästä saatu tilaajakohtainen autentikointi-informaatio käsittää lisäksi avaimen (Kc), jolloin tilaaja rekisteröidään Kerberos-järjestelmän asiakkaaksi siten, että avain rekisteröidään (a) asiakkaan salasanana ja (b) salasanana palveluun, joka muodostetaan asiakkaan IP-osoitteelle tai matkaviestinjärjestelmässä käytettävälle tilaajatunnukselle (IMSI).

6. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tilaajan autentikointi-informaatio haetaan erillisen proxy-palvelimen (HP) avulla, joka toimii matkaviestinjärjestelmän vierailijarekisteriä VLR emuloivana verkkoelementtinä, joka pyytää autentikointi-informaation tilaajan kotirekisterin HLR yhteydessä olevasta tunnistuskeskuksesta AuC samalla tavalla kuin matkaviestinjärjestelmän oma vierailijarekisteri.

7. Patenttivaatimuksen 1 mukainen menetelmä, t u n n e t t u siitä, että tilaajan autentikointi-informaatio haetaan erillisen proxy-palvelimen (BP) avulla, joka toimii matkaviestinjärjestelmän tukiasemaohjainta emuloivana verkkoelementtinä, joka on yhteydessä matkaviestinjärjestelmän matkaviestinkeskukseen (MSC) autentikointi-informaation hakemiseksi tilaajan kotirekisterin HLR yhteydessä olevasta tunnistuskeskuksesta AuC samalla tavalla kuin autentikointi-informaatio haetaan matkaviestinjärjestelmän omaan tukiasemaohjaimeen.

8. Autentikointijärjestelmä tietoliikenneverkkoja, erityisesti IP-verkkoja varten, joka järjestelmä käsittää todennuselimet verkkoon kytkeytyneen tilaajan identiteetin todentamiseksi, t u n n e t t u siitä, että todennuselimet käsittävät

- verkon päätelaitteeseen (TE1) kytketyn tilaajan tunnistusyksikön (SIM), joka on oleellisesti samanlainen kuin erillisessä matkaviestinjärjestelmässä (MN) käytettävä tilaajan tunnistusyksikkö ja jolle syötteenä annetusta haasteesta voidaan määrittää vaste,
- ilmoituselimet (HA) ilmoituksen antamiseksi päätelaitteen kytkeytyessä verkkoon,
- erityisen turvapalvelimen (SS) mainitun ilmoituksen vastaanottamiseksi,
- elimet tilaajaa vastaavan autentikointi-informaation pyytämiseksi mainitusta matkaviestinjärjestelmästä (MN), joka informaatio sisältää ainakin haasteen ja vasteen, ja
- mainitun verkon puolella tiedonsiirto- ja tarkastuselimet mainitun haasteen lähettämiseksi verkon kautta tunnistusyksikölle, vasteen palauttamiseksi päätelaitteelta verkolle ja saadun vasteen vertaamiseksi matkaviestinjärjestelmästä saatuun vasteeseen.

9. Patenttivaatimuksen 8 mukainen järjestelmä, t u n n e t t u siitä, että mainittu tunnistusyksikkö on GSM-verkossa käytettävä tunnistusyksikkö (SIM).

10. Patenttivaatimuksen 8 mukainen järjestelmä, t u n n e t t u siitä,

että ilmoituselimet on sovitettu mobile IP -verkon mukaiseen kotiagenttiin (HA).

11. Patenttivaatimuksen 8 mukainen järjestelmä, t u n n e t t u siitä, että elimet autentikointi-informaation pyytämiseksi käsittävät mainitun turvapalvelimen ja proxy-palvelimen (HP, BP), joka on kytketty GSM-verkkoon.

12. Patenttivaatimuksen 11 mukainen järjestelmä, t u n n e t t u siitä, että proxy-palvelin toimii GSM-verkon vierailijarekisteriä VLR emuloivana verkkoelementtinä.

13. Patenttivaatimuksen 11 mukainen järjestelmä, t u n n e t t u siitä, että proxy-palvelin toimii GSM-verkon tukiasemaohjainta BSC emuloivana verkkoelementtinä.

14. Patenttivaatimuksen 11 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmä käsittää lisäksi sinänsä tunnetun Kerberos-palvelimen (KS), jonka käyttäjäksi tilaaja rekisteröidään onnistuneen autentikoinnin seurauksena.

15. Autentikointimenetelmä tietoliikenneverkkoja, erityisesti IP-verkkoja varten, jonka menetelmän mukaisesti todennetaan verkkoon kytkeytyneen tilaajan identiteetti, t u n n e t t u siitä, että

- verkon päätelaitteessa (TE1) käytetään oleellisesti samanlaista tilaajan tunnistusyksikköä (SIM) kuin tunnetussa matkaviestinjärjestelmässä (MN), joka tunnistusyksikkö on sellainen, että sille syötteenä annetusta haasteesta saadaan tuloksena vaste,

- talletetaan tietokantaan (DB) tilaajakohtaista autentikointi-informaatiota, joka on siten oleellisesti samanlaista kuin mainitussa matkaviestinjärjestelmässä autentikointiin käytettävä informaatio, että se sisältää ainakin haasteen ja vasteen,

- verkossa käytetään lisäksi erityistä turvapalvelinta (SS) siten, että päätelaitteen kytkeytyessä verkkoon turvapalvelimelle lähetetään ilmoitus uudesta käyttäjästä,

- vasteena ilmoitukselle haetaan uutta käyttäjää vastaavan tilaajan autentikointi-informaatio mainitusta tietokannasta (DB), ja

- autentikointi suoritetaan tietokannasta saadun autentikointi-informaation perusteella lähettämällä verkon kautta mainittu haaste päätelaitteelle, generoimalla päätelaitteen tunnistusyksikössä haasteesta vaste ja vertaamalla vastetta tietokannasta saatuun vasteeseen.

16. Patenttivaatimuksen 15 mukainen menetelmä, t u n n e t t u siitä, että tietokanta talletetaan turvapalvelimen yhteyteen.

17. Patenttivaatimuksen 15 mukainen menetelmä, t u n n e t t u siitä,

että vasteena onnistuneelle autentikoinnille suoritetaan tilaajan rekisteröinti erillisen avainten hallintajärjestelmän käyttäjäksi.

18. Patenttivaatimuksen 17 mukainen menetelmä, t u n n e t t u siitä, että avainten hallintajärjestelmänä käytetään tunnettua Kerberos-järjestelmää.

19. Autentikointijärjestelmä tietoliikenneverkkoja, erityisesti IP-verkkoja varten, joka järjestelmä käsittää todennuselimet verkkoon kytkeytyneen tilaajan identiteetin todentamiseksi, t u n n e t t u siitä, että todennuselimet käsittävät

- verkon päätelaitteeseen (TE1) kytketyn tilaajan tunnistusyksikön (SIM), joka on oleellisesti samanlainen kuin erillisessä matkaviestinjärjestelmässä (MN) käytettävä tilaajan tunnistusyksikkö ja jolle syötteenä annetusta haasteesta voidaan määrittää vaste,

- ilmoituselimet (HA) ilmoituksen antamiseksi päätelaitteen kytkeytyessä verkkoon,

- erityisen turvapalvelimen (SS) mainitun ilmoituksen vastaanottamiseksi,

- tietokantaelimet (SS, DB), jotka käsittävät tietokannan (DB), johon on talletettu tilaajakohtaista autentikointi-informaatiota, joka on siten oleellisesti samanlaista kuin mainitussa matkaviestinjärjestelmässä autentikointiin käytettävä informaatio, että se sisältää ainakin haasteen ja vasteen, ja hakuelimet (SS) tilaajan autentikointi-informaation hakemiseksi mainitusta tietokannasta vasteena ilmoitukselle,

- mainitun verkon puolella tiedonsiirto- ja tarkastuselimet mainitun haasteen lähettämiseksi verkon kautta tunnistusyksikölle, vasteen palauttamiseksi päätelaitteelta verkolle ja saadun vasteen vertaamiseksi tietokannasta saatuun vasteeseen.

20. Patenttivaatimuksen 19 mukainen järjestelmä, t u n n e t t u siitä, että mainittu tunnistusyksikkö on GSM-verkossa käytettävä tunnistusyksikkö (SIM).

21. Patenttivaatimuksen 19 mukainen järjestelmä, t u n n e t t u siitä, että ilmoituselimet on sovitettu mobile IP -verkon mukaiseen kotiagenttiin (HA).

22. Patenttivaatimuksen 19 mukainen järjestelmä, t u n n e t t u siitä, että järjestelmä käsittää lisäksi sinänsä tunnetun Kerberos-palvelimen (KS), jonka asiakkaaksi tilaaja rekisteröidään onnistuneen autentikoinnin seurauksena.

(57) Tiivistelmä

Keksintö koskee tietoliikenneverkossa, erityisesti IP-verkossa suoritettavaa autentikointia. Jotta IP-verkkojen käyttäjät saataisiin autentikoitua yksinkertaisesti ja joustavasti maantieteellisesti laajalla alueella, IP-verkon päätelaitteessa (TE1) käytetään erillisessä matkaviestinjärjestelmässä (MN) käytettävää tilaajan tunnistusyksikköä (SIM), jolle syötteenä annetusta haasteesta voidaan määrittää vaste. IP-verkossa on lisäksi erityinen turvapalvelin (SS), jolle lähetetään ilmoitus uudesta käyttäjästä tilaajan kytkeytyessä IP-verkkoon. Tilaajan autentikointi-informaatio, joka sisältää ainakin haasteen ja vasteen, haetaan mainitusta matkaviestinjärjestelmästä IP-verkkoon ja autentikointi suoritetaan matkaviestinjärjestelmästä saadun autentikointi-informaation perusteella lähettämällä IP-verkon kautta mainittu haaste päätelaitteelle, generoimalla päätelaitteen tunnistusyksikössä haasteesta vaste ja vertaamalla vastetta matkaviestinjärjestelmästä saatuun vasteeseen. Järjestelmässä voidaan käyttää myös tietokantaa (DB), jonne tilaajakohtaista autentikointi-informaatiota talletetaan etukäteen, jolloin ko. informaatiota ei tarvitse hakea matkaviestinjärjestelmästä tilaajan kytkeytyessä verkkoon.

(kuvio 1)

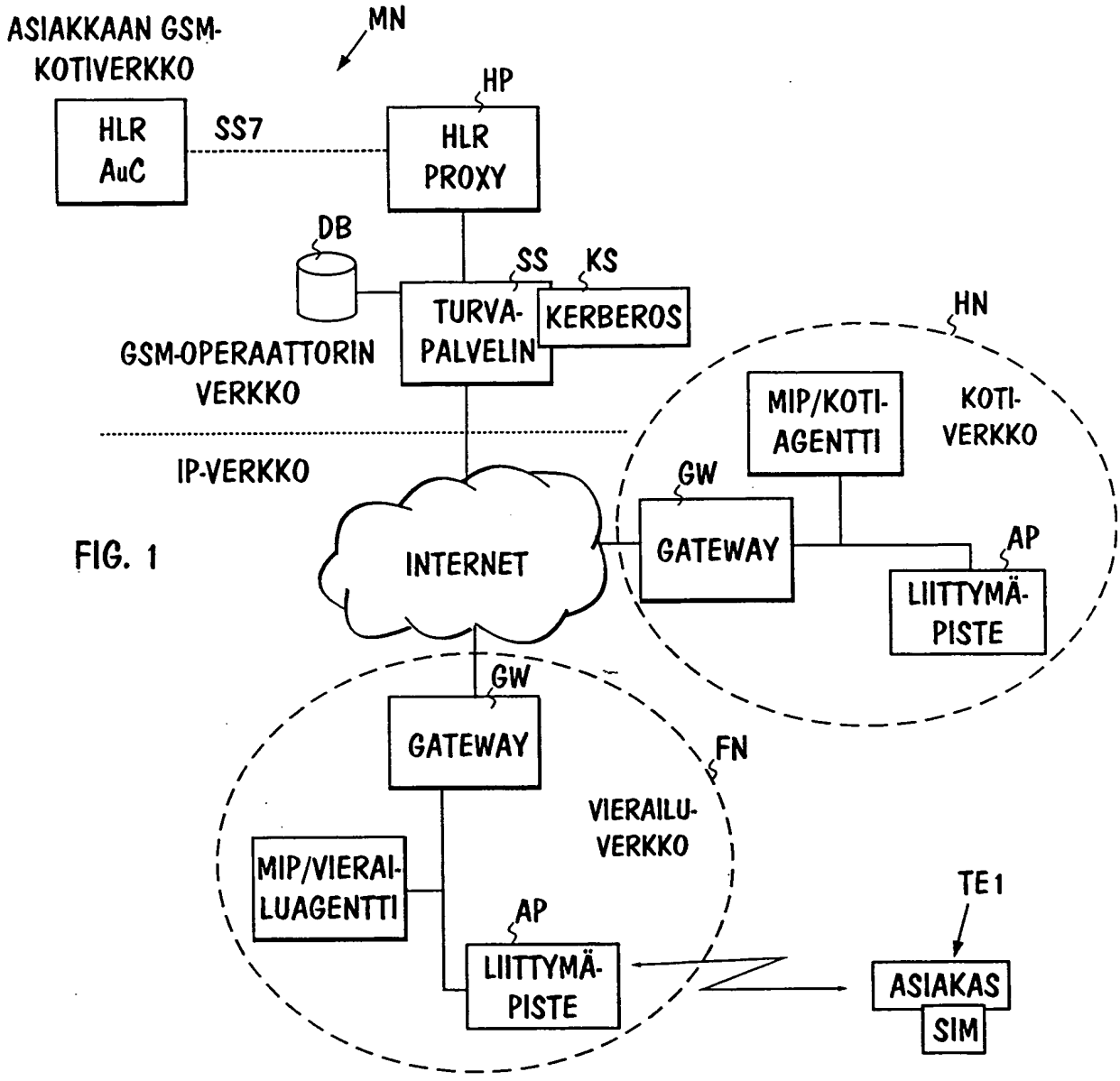

ASIAKKAAN GSM-
KOTIVERKKO
MN
HP
HLR
AuC
SS7
HLR
PROXY
DB
SS
KS
TURVA-
PALVELIN
KERBEROS
GSM-OPERAATTORIN
VERKKO
HN
MIP/KOTI-
AGENTTI
KOTI-
VERKKO
IP-VERKKO
GW
GATEWAY
AP
LIITTYMÄ-
PISTE
INTERNET
GW
GATEWAY
FN
VIERAILU-
VERKKO
MIP/VIERAI-
LUAGENTTI
AP
LIITTYMÄ-
PISTE
TE1
ASIAKAS
SIM

FIG. 1

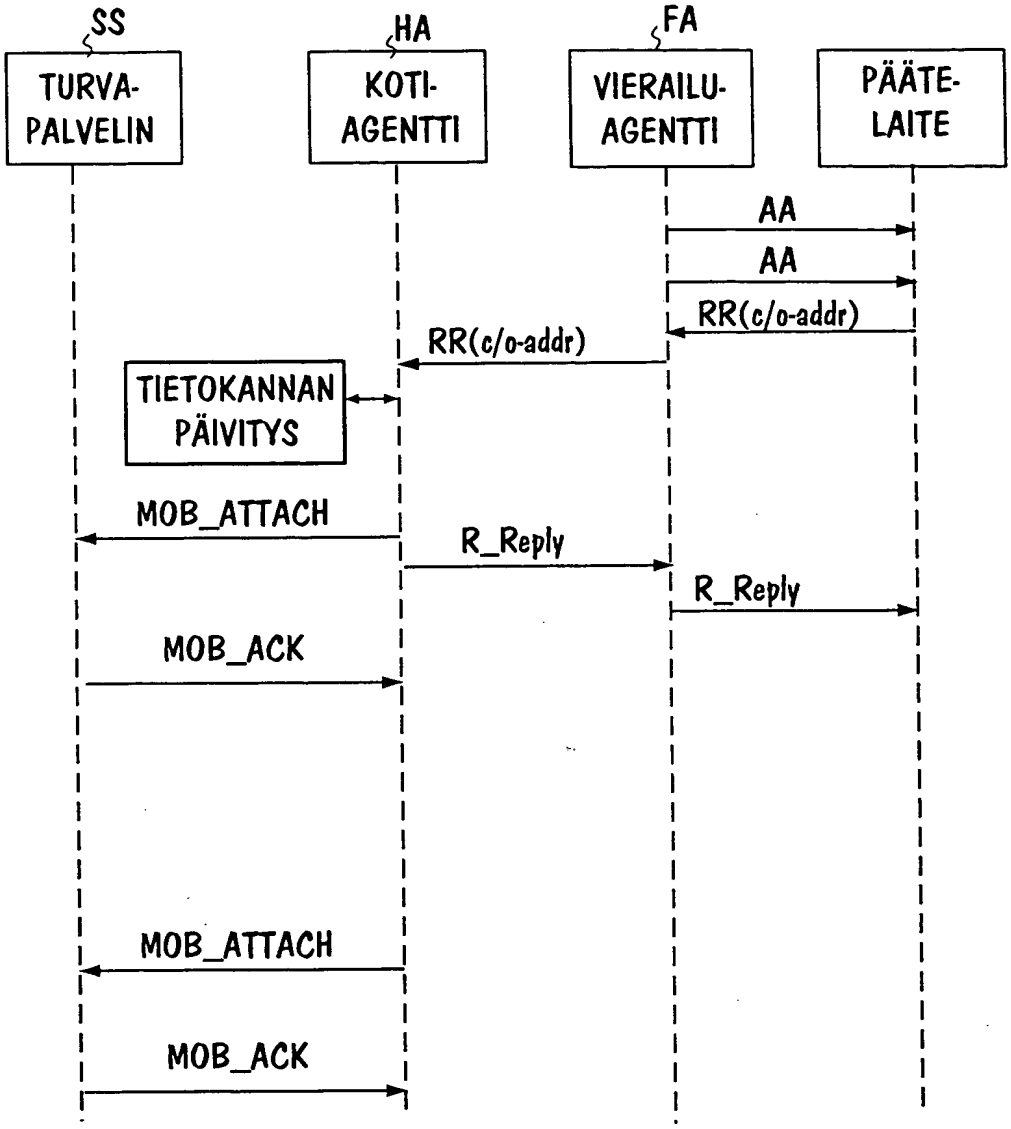

SS
HA
FA
TURVA-PALVELIN
KOTI-AGENTTI
VIERAILU-AGENTTI
PÄÄTE-LAITE
AA
AA
RR(c/o-addr)
RR(c/o-addr)
TIETOKANNAN PÄIVITYS
MOB_ATTACH
R_Reply
R_Reply
MOB_ACK
MOB_ATTACH
MOB_ACK

FIG. 2

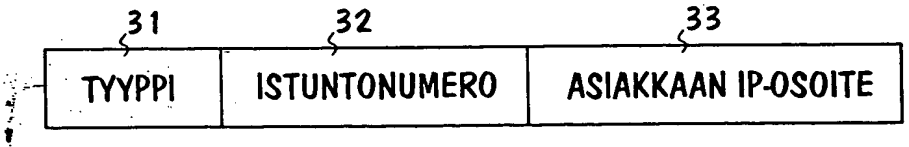

31
32
33
TYYPPI
ISTUNTONUMERO
ASIAKKAAN IP-OSOITE

FIG. 3

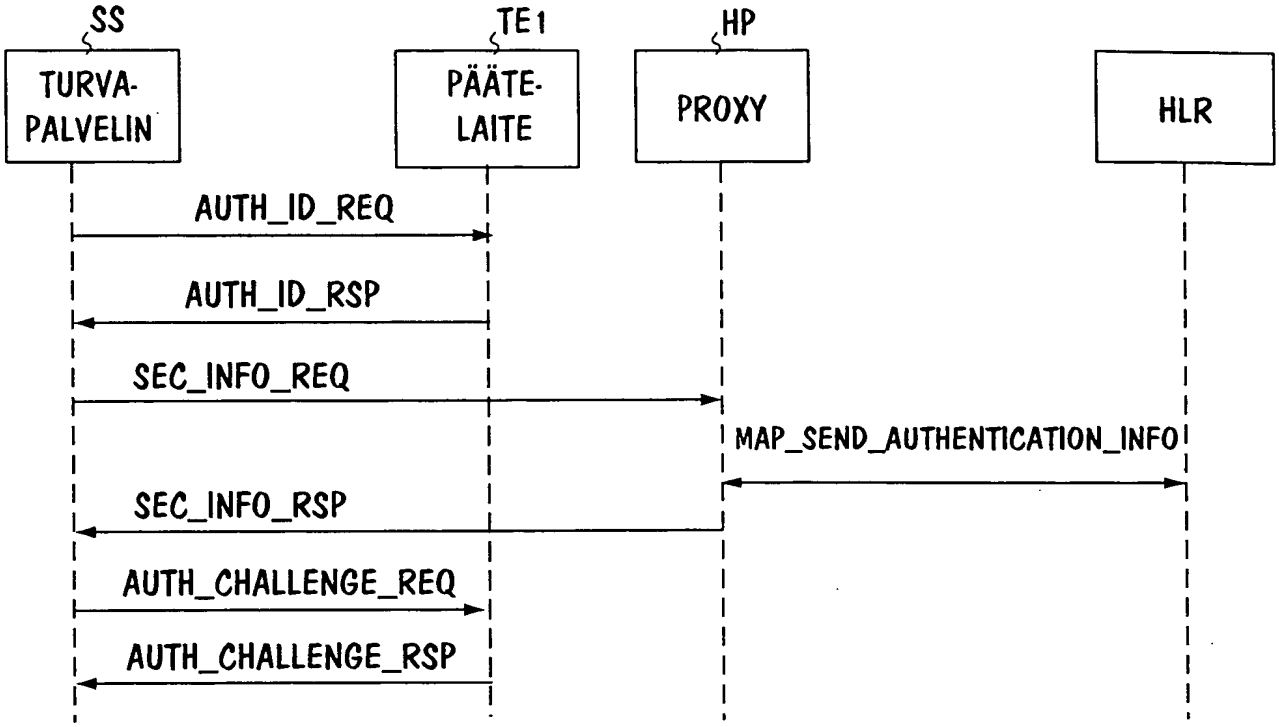


FIG. 4

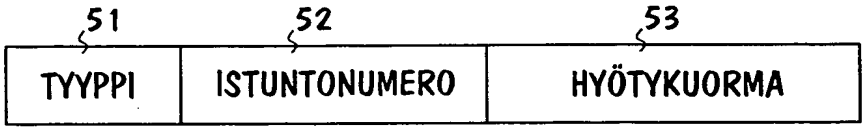


FIG. 5

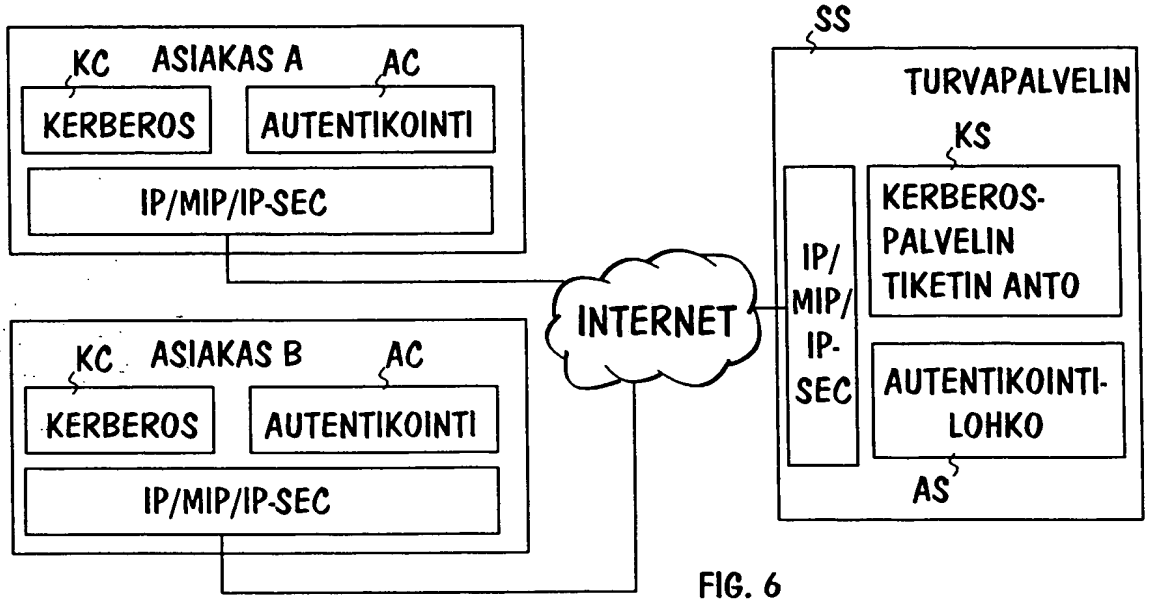


FIG. 6

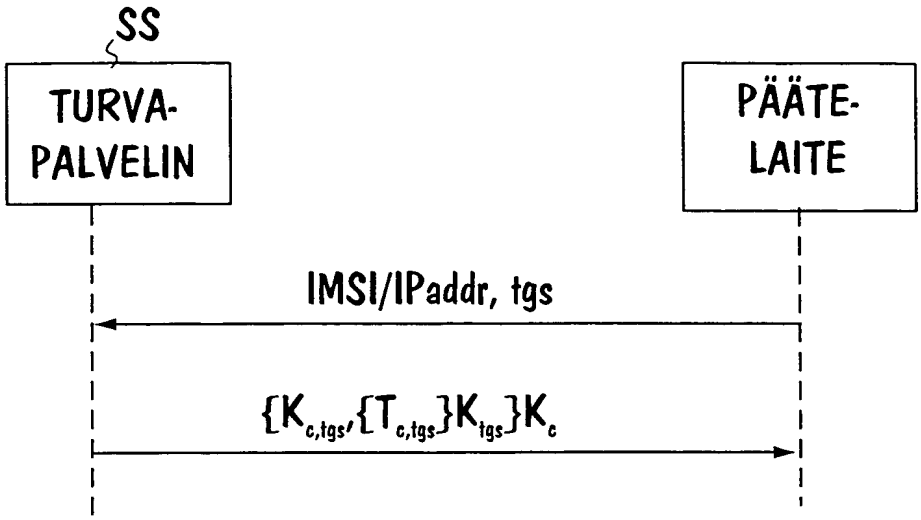


FIG. 7

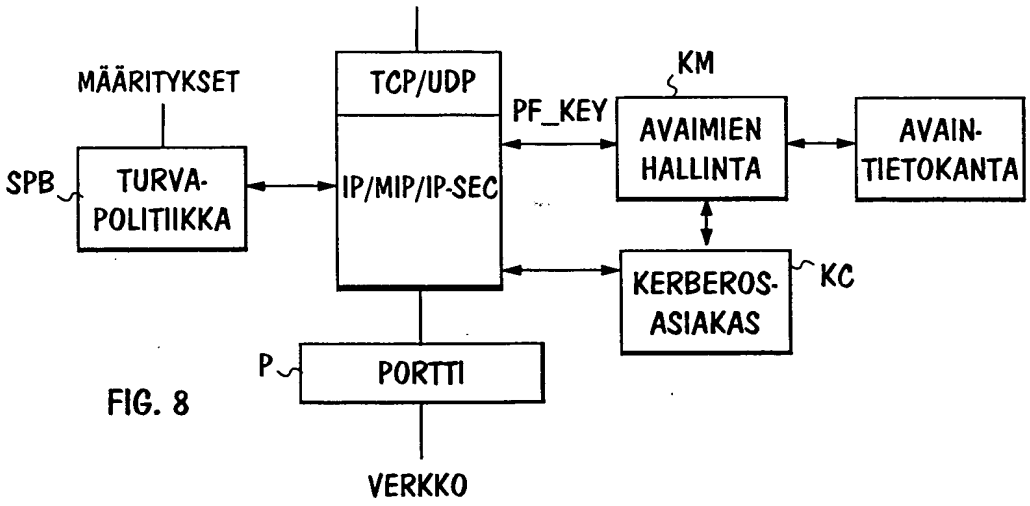


FIG. 8

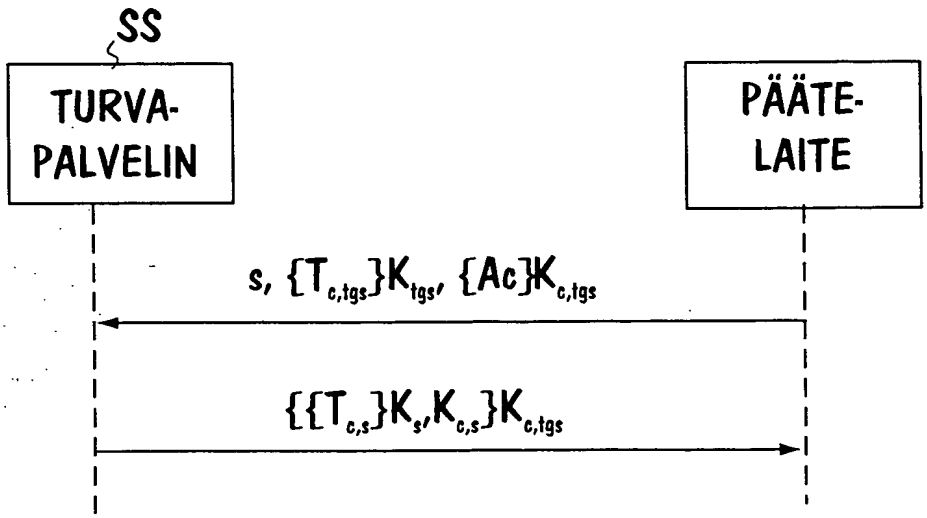


FIG. 9

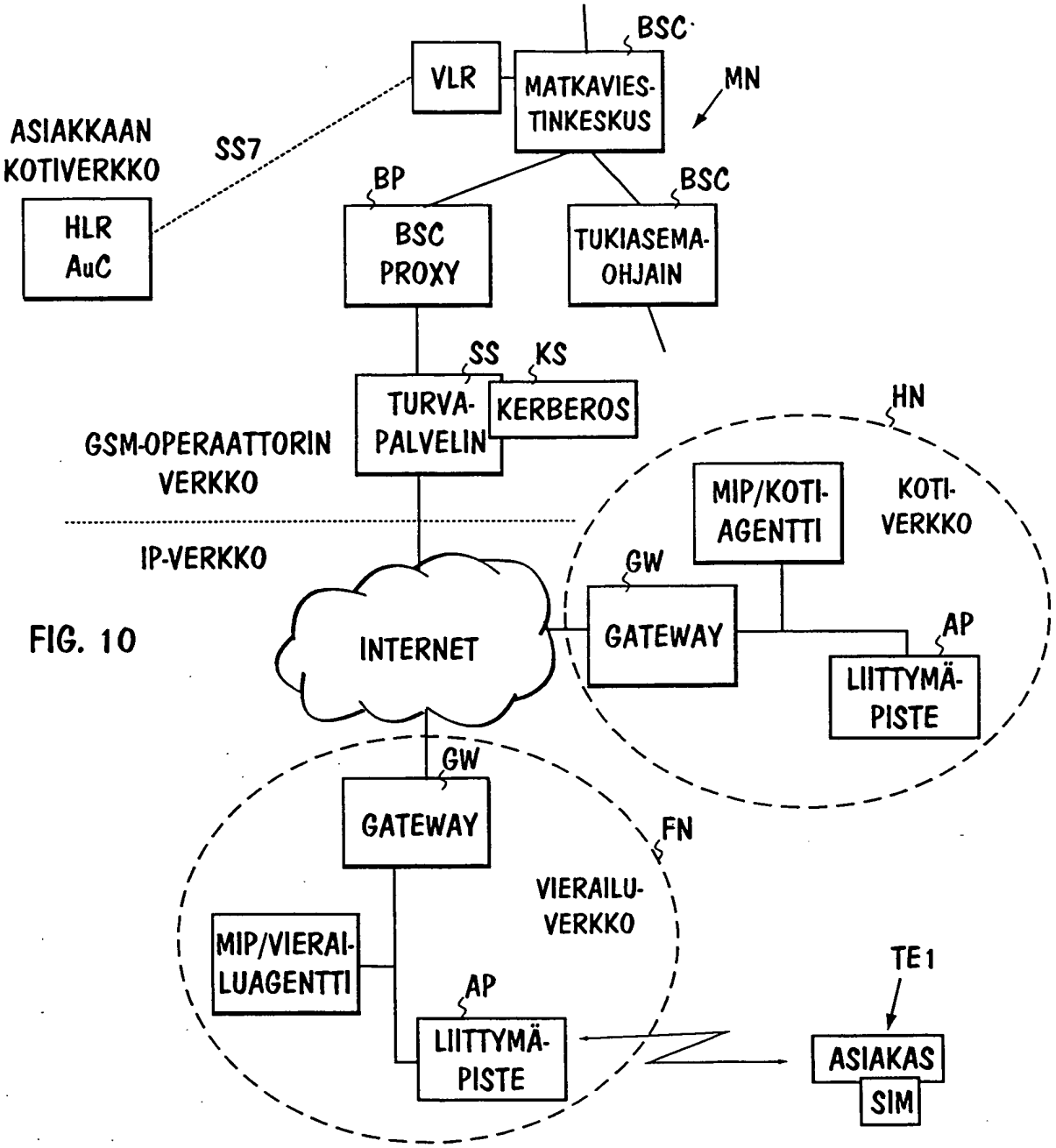

BSC
VLR
MATKAVIES-
TINKESKUS
MN
ASIAKKAAN
KOTIVERKKO
SS7
HLR
AuC
BP
BSC
BSC
PROXY
TUKIASEMA-
OHJAIN
SS
KS
TURVA-
PALVELIN
KERBEROS
HN
GSM-OPERAATTORIN
VERKKO
MIP/KOTI-
AGENTTI
KOTI-
VERKKO
IP-VERKKO
GW
INTERNET
GATEWAY
AP
LIITTYMÄ-
PISTE
GW
GATEWAY
FN
VIERAILU-
VERKKO
MIP/VIERAI-
LUAGENTTI
AP
LIITTYMÄ-
PISTE
TE1
ASIAKAS
SIM

FIG. 10

THIS PAGE BLANK (USPTO)